Online Safety Policy

St. Mary's CE Primary School

Approved by: Elizabeth Green	**Date:** September 2024
Last reviewed on:	September 2024
Next review due by:	September 2025

Elements
Diocesan Learning Trust

Instilling a life-long love for learning in an inclusive, supportive Christian community.

Vision and Values

OUR VISION:

At St Mary's we aim to nurture the whole child, with the opportunity to develop their full potential through an inspiring and creative curriculum, instilling a life-long love for learning in an inclusive, supportive Christian community. Providing them with the strength to enable them to flourish.

Isaiah 40:31

But those who trust in the Lord for help, will find their strength renewed.

They will rise on wings like eagles;

They will run and not grow weary;

They will walk and not grow weak.

OUR VALUES:

At St Mary's CE Primary School, these values are at the heart of everything we do at school. We actively teach these values to children through our curriculum, collective worship and our day to day interactions with children. We always encourage children to reflect these values in their own behaviour in school and in the wider community.

LOVE is the most important core value in our school. We strive to bring our community together through love, kindness and friendship. We seek to appreciate everyone for who they are and welcome them to our school family. We encourage the whole school community to consider others before themselves and to practice friendship, compassion, forgiveness and tolerance.

HOPE is rooted in God's love for us. At St Mary's, we have high hopes and aspirations for all our pupils, our school and our community

TRUST is central to our school community. We trust in God, one another and ourselves. We value those around us who we know we can rely on, who can support and be there for us. When we work together, we grow stronger and are enriched.

RESPECT, one of our core Christian values, includes self-respect, respect for each other, the wider community and the world. Respect embraces individual differences and similarities within **school and** community. We celebrate these differences and rejoice in similarities. As a school, we ensure children have equal opportunities to be successful and appreciate everyone's talents.

PERSEVERANCE, at St Marys we work hard and aim to be the best we can. We know that sometimes things can be difficult, but we keep going and with God's help we don't give up.

FRIENDSHIP, friends are incredibly important as children grow up. Friendships allow children to grow and develop social and emotional skills. This ensures that the unique individuality of each person is recognised echoing the value placed by God on the preciousness of each person.

Everyone in the school community has a part to play in achieving strong, meaningful relationships and excellent behaviour. We all have a shared responsibility to provide the very best learning environment for our children and so we have a set of principles that apply to everyone (appendix 1).

Aims

The purpose of our online safety policy is to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that St. Mary's CE Primary School is a safe and secure environment.
- Raise awareness with all members of St. Mary's CE Primary School regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

This policy applies to all staff including the Local School Committee, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers. This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones. This policy must be read in conjunction with other relevant school policies including child protection, behaviour, anti-bullying, learning policy, data protection, and Relationships and Health Education.

Procedures

The Four Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

The policy takes into account the National Curriculum computing programmes of study.

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

This policy adheres to the principles under data protection law and the Data Protection Act. For further information, please review the school's data protection policy published on the school's website.

Roles and responsibilities:

The Local School Committee (LSC)

The LSC has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The LSC will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LSC will also make sure all staff receive regular online safety updates (via email and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LSC will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The LSC should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The LSC must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL)and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and Local School Committee to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Local School Board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT manager (currently the Headteacher)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to

assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the DSL or deputy or contacting via phone or email
- Following the correct procedures by prior consent from the Headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendix 2)
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

- Role modelling safe and appropriate uses of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Notify a member of staff or the Headteacher if any concerns or queries regarding this policy.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

Pupils

Pupils are expected to:

- Take responsibility for keeping themselves and others safe online.
- Assess the personal risks of using technology, behaving safely and responsibly to limit those risks.
- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
- Understand and 'sign up' to the Acceptable Use Agreement for pupils (see appendix 2).

Online Safety Education:

Education of Pupils

Pupils will be taught about online safety in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned online safety teaching begins every September during induction and continues to be provided as part of computing and other curriculum areas and will be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school.
- The requirements set out for 'Relationships Education and Health Education' which includes aspects of online safety.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.

- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement (see appendix 2) and be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

<u>Education of Parents and Carers</u>

Parents and carers play an essential role in the education of their children and in the monitoring of children's online experiences. We will seek to provide information and awareness to parents and carers through:

- Newsletters
- Emails
- Parents' Evenings (where necessary)
- Meetings with the Headteacher/DSLs (where necessary)

This policy will also be shared with parents/carers via our website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and/or Headteacher/Deputy Headteacher.
Concerns or queries about this policy can be raised with the Headteacher.

Education and Training of Staff

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is *repeated negative behaviour that is intended to make others feel upset, uncomfortable or unsafe*. Cyber-bullying can be carried out by an individual or a group of people towards another individual or group, where the bully or bullies hold more power than those being bullied.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying where appropriate within the curriculum. This includes RHE lessons (Relationships and Health Education) and other subjects where appropriate. The issue may also be address in assemblies and by our Anti-Bullying Ambassadors.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure that the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

<u>Examining Electronic Devices</u>

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied hat they have reasonable grounds for suspecting any of the above, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or a DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or

- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial Intelligence (AI):

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St. Mary's CE Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St. Mary's CE Primary School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by school.

Acceptable Use:

Information System Security and Data Protection

St. Mary's CE Primary School is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

St. Mary's CE Primary School use RM Dudley Grid for Learning. We will liaise with DGfL to ensure regular reviews take place and software is in place to guard against access to and to highlight any person accessing inappropriate sited or information. We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act. All users will be provided with a username and password. The Headteacher has overall responsibility for internet safety and will have access to all email addresses and passwords provided. Users will be responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must ensure that they correctly log-off from a computer terminal after accessing personal data. Users must immediately report any suspicion or evidence that there has been a breach of security.

Staff should not remove personal or sensitive data from the school premises without permission of the Headteacher. Any data which is impractical to ensure is kept in school, e.g. reports, will be kept secure, by use of encrypted memory sticks which are password protected.

Every effort is made to encourage pupils not to give out their personal details, phone number, school, home address, computer passwords, etc.

Acceptable use of the Internet in School

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. At St. Mary's CE Primary School, internet access will be designed to enhance and extend education.

All pupils, parents, staff, governors and volunteers (where appropriate) are expected to sign an agreement regarding the acceptable use of the school's ICT systems and internet (see appendices 1 and 2). Visitors will be expected to read and agree with the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, governors, volunteers and visitors (where relevant) to ensure they comply with the above and restrict access through filtering and monitoring systems where appropriate.

Where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use. Where pupils can freely search the internet, staff should be vigilant in monitoring the content of the websites, encouraging responsible use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. They will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the Headteacher. Where possible, appropriate action will be taken to block further access. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access, inappropriate materials.

All school owned devices will be used in accordance with the school Acceptable Use Statement (see appendices 1 and 2) and with appropriate safety and security measure in place.

More information is set out in the acceptable use agreements in appendices 1 and 2.

Use of Digital and Video Images

When using images and videos, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet; their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment of individuals. We aim to inform and educate users about their risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff to educate pupils about the risks associated with taking and sharing images. They should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff can take digital/video images to support educational aims but must follow school policy concerning the sharing, distribution and publication of those images. Images should only be taken using school equipment. Under no circumstances should personal equipment of staff be used for such purposes.
- Permission from parents/carers will always be obtained before images/videos/work of pupils are electronically published.
- Pupils' full names will not be used anywhere on the website.

Use of Email

The school email service is safe, secure and is monitored. All members of staff are provided with a specific school email address to use for any official communication. The use of personal email addresses by staff for any official school business is not permitted. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be. Members of the community must immediately tell the designated safeguarding lead if they receive offensive communication and this will be recorded in the school safeguarding records. School email addresses and other official contact details will not be used for setting up personal social media accounts. Staff will be encouraged to develop an appropriate work life balance when responding to email.

Pupils may only use school provided email accounts/Purple Mash email accounts for educational purposes and must immediately tell a teacher if they receive an offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

School Website

We will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

Social Media

Expectations regarding safe and responsible use of social media will apply to all members of St. Mary's CE Primary School and exist to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others. All members of St. Mary's CE Primary School are expected to engage in social media in a positive, safe and responsible manner at all times. All members are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others. The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems

Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Statement (see appendix 1).
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- Any concerns regarding the online conduct of any member of St. Mary's CE Primary School on social media sites should be reported to the Headteacher and will be managed in accordance with policies such as allegations against staff, behaviour and safeguarding.

Pupil Use of Social Media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Agreement (see appendix 2).
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including the behaviour policy.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

Mobile Phones and Personal Devices

The widespread ownership of mobile phones and range of other personal devices among children, young people and adults will require all members of St. Mary's CE Primary School to take steps to ensure that mobile phones and personal devices are used responsibly.

Pupils are not allowed to bring mobile phones and other devices, such as smart watches and/or fitness trackers into school. If a child does bring a phone or device onto the school site, it is handed in to the school office where the parents/carers will have responsibility for retrieving it. The exception to this is: Year 6 pupils may bring to school a mobile device if they are walking to and from school on their own. It must be handed to their class teacher who will store securely in the classroom cupboard for the duration of the day. Devices must be switched off.

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Mobile phones and personal devices are not permitted to be used around school by staff except for the designated areas. Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose. Staff wearing smart watches must ensure that communications for the watch are disabled during their time at school.

Staff using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1. Staff members must take appropriate steps to ensure that their device remains secure. This includes, but is not limited to:

- Their work device is secure and password-protected, and that they do not share their password with others. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- They must take all reasonable steps to ensure the security of their work device when using it outside school, including not sharing the device among family and friends
- Making sure the device locks if left inactive for a period of time
- Ensuring anti-virus and anti-spyware software is up to date
- Keeping operating systems up to date by always installing the latest updates

The preferred option of storing documents and data is through One Drive or Teams.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, the pupil may be spoken to regarding the rules of acceptable use of ICT systems and internet in school, banned from using devices in school for a set period of time and/or parents/carers informed. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Headteacher and shared with the Quality of Education Committee of the Local School Committee. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with Other Polices

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Relationships and Health Education Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Staff Code of Conduct
- Mobile Phone Policy

- Appendix 1 – Staff Acceptable Use Statement

Acceptable Use Statement

For Staff & Adult Users

The computer systems within school are made available to students, staff and other adults as tools for learning and to enhance professional activities including teaching, research, administration and management. The school's Acceptable Use Statement has been drawn up to protect all parties – the students, the staff, other adults and the school and are reviewed on a regular basis.

Staff and other adults wishing to use the school's computer systems, email or internet should sign a copy of this Acceptable Use Statement and return it to the Headteacher for approval.

For my professional and personal safety:

- I understand that ST. MARY'S CE PRIMARY SCHOOL will monitor my use of the school digital technology and communication systems.
- I understand that rules set out in this agreement also apply to use of these technologies out of school and to the transfer of personal data out of school.
- I understand that school digital technology systems are primarily intended for educational use. All internet activity should be appropriate to the student's education. Use for personal financial gain, gambling, political purposes or advertising is forbidden. Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- I will not use the device in any way which could harm the school's reputation.
- I will not access any social networking sites or chat rooms.
- I will not promote private businesses unless that business is directly related to the school.
- I understand that access should only be made via the authorised account and password, which should not be made available to any other person. I understand that I am responsible for all activity carried out under my username.
- I will immediately report any illegal, inappropriate or harmful material to the Headteacher.
- When I use my mobile devices in school I will follow the rules set out in the online safety policy, in the same way as if I was using ST. MARY'S CE PRIMARY SCHOOL equipment.
- I will not take photographs or videos of pupils without checking with teachers first (if governor, volunteer or visitor)
- I will not engage in any online activity that may compromise my professional role or responsibilities, for example social media. No reference of ST. MARY'S CE PRIMARY SCHOOL should be made on any social networking site.
- I understand that this Acceptable Use Statement applies not only to my work and use of ST. MARY'S CE PRIMARY SCHOOL systems but also applies to my use of ST. MARY'S CE PRIMARY SCHOOL systems off the premises and my use of personal equipment on the premises or in situations related to my employment by ST. MARY'S CE PRIMARY SCHOOL.

I will be professional in my communications and actions when using ST. MARY'S CE PRIMARY SCHOOL ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will only use the approved email system for school business.
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for the letters or other media. I am responsible for all email sent and for contacts made that may result in email being received.
- I will not use my personal devices to take photographs/record videos related to school business.
- I will not engage in any on-line activity that may compromise my professional responsibilities. Posting anonymous messages and forwarding chain letters is forbidden.

To ensure safe and secure access to technologies and to ensure the smooth running of ST. MARY'S CE PRIMARY SCHOOL:

- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden. I will not open any hyperlinks in emails or attachments to emails unless the source is known and trusted.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will try not to use any programmes or software that might allow me to bypass the filtering systems in place.
- I will not install programmes of any type on a machine.
- Copyright of materials must be respected.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the data policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.

Misuse of the school's computer equipment, email or the internet are serious offences. Research Machines (RM) has a contractual obligation to monitor the use of the email and internet services provided as part of the DGfL, this information may be recorded and may be used in disciplinary procedures if necessary. RM, the Council and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

Acceptable Use Agreement

I have read the above statement and agree to abide by the conditions. I understand that misuse of schools computer systems, email or the internet are serious offences and could lead to disciplinary procedures, up to and including dismissal.

Full name (please print) ……..

Signed …… Date ……

Headteacher …… Date ……

Appendix 2 – Pupil Acceptable Use Agreement

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

All children at St. Mary's CE Primary are responsible for following school rules and values when using computers and other electronic devices.

When using the school's ICT systems and accessing the internet in school, to keep myself safe:

- I will use computers and devices for learning activities only
- I will use computers and devices with a teacher being present, or with a teacher's permission
- I will keep my username and password secure. I will not share it and I will not try to use any other person's username and password.
- I will never give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
- I will ask for help if I get lost on the internet
- I will immediately let an adult know if I discover anything which makes me feel upset or uncomfortable
- I will always log off or shut down a computer when I'm finished working on it
- If I accidentally damage any equipment, I will tell a teacher immediately
- I will only send emails that my teacher has approved so that they can be sure I am kept safe
- I will not log into the school's network using someone else's details
- I will not look at other people's files or delete other people's files without permission
- I will not access any websites I know to be inappropriate
- I will not access social networking sites or chat rooms (unless my teacher has expressly allowed this as part of a learning activity)
- I will not open any attachments, follow any links in pop-up boxes or emails or download any files, without first checking with a teacher
- I will not use any inappropriate language when using computers, including in search bars, in documents and in emails

If I bring a personal mobile phone or other personal electronic device (e.g. smart watch/fitness tracker) into school:

- I will tell a teacher immediately and take the device to the school office, where it will be stored securely
- I know that a parent/career will be required to collect the device at the end of the school day from the office

I know that the school will monitor all usage of computers, including the websites I visit, what I search for using search engines and what I type into documents.

I know that if I do not follow these directions when using computers/devices I might not be able to use school computers/devices for a period of time and my parents/carers may be contacted.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials and that the school cannot

be held responsible for the nature or content of materials accessed through the internet and mobile technologies. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/carer):	**Date:**